BURSOR & FISHER, P.A.
L Timothy Fisher (State Bar No. 191626)
Joel D. Smith (State Bar No. 244902)
1990 North California Blvd., Suite 940
Walnut Creek, CA 94596
Telephone: (925) 300-4455
Facsimile: (925) 407-2700
E-mail: ltfisher@bursor.com
jsmith@bursor.com

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

AUDRA GRAHAM and STACY MOISE, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

NOOM INC. and FULLSTORY, INC.,

Defendants.

Case No. 3:20-cv-06903-LB

PLAINTIFFS' OPPOSITION TO NOOM'S MOTION TO DISMISS THE FIRST AMENDED COMPLAINT

Date: Apr. 8, 2021
Time: 9:30 a.m.
Courtroom: B, 15th Floor
Judge: Hon. Laurel Beeler

TABLE OF CONTENTS

PAGE(S)

TABLE OF AUTHORITIES

PAGE(S)

CASES

STATUTES

RULES

INTRODUCTION

Noom hired FullStory to secretly record everything anyone does on its website, noom.com, using a tool called "Session Replay." With this tool, Defendants "watch and record a visitor's every move on a website, in real time" with FullStory's software providing "pixel-perfect playback." FAC ¶ 20, 22-27. Defendants also can monitor website visitors *live* where (in FullStory's own words) "you'll essentially be riding along in near real time." *Id.* at ¶ 30. This technology is not normal, not safe, and "far exceeds user expectations." FAC ¶ 55; *see also id.* at ¶¶ 28, 34. It also violates California's privacy and wiretap laws. Noom's motion to dismiss should be denied in its entirety.

First, most of Noom's arguments concerning the wiretapping claim under Cal. Penal Code § 631(a) are rebutted by *Revitch v. New Moosejaw, LLC*, 2019 WL 5485330 (N.D. Cal. Oct. 23, 2019), which involved very similar facts, and two Ninth Circuit decisions addressing the monitoring of internet activity: *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589 (9th Cir. 2020), and *In re Zynga Privacy Litig.*, 750 F.3d 1098 (9th Cir. 2014).

Second, Noom argues Plaintiffs lack standing to sue under Cal. Penal Code § 635, and that they cannot be liable in any event because the technology is not "primarily or exclusively designed or intended for eavesdropping." These arguments are contradicted by the plain language of the statute, as well as the outcome in *Moosejaw* and the Sixth Circuit's decision in *Luis v. Zang*, 833 F.3d 619 (6th Cir. 2016). At best, Noom's arguments that FullStory's software is not a "device" within the meaning of § 635 involve factual disputes that cannot be resolved on a 12(b)(6) motion.

Third, the question of whether surreptitiously recording website activity is egregious enough to support a common law invasion of privacy claim is a question of fact. *See In re Facebook*, 956 F.3d at 607 ("The ultimate question of whether Facebook's tracking and collection practices could highly offend a reasonable individual is an issue that cannot be resolved at the pleading stage.").[1]

[1] In its Introduction, Noom lays it on a bit thick with hyperbolic attacks on Plaintiffs' counsel for engaging in a campaign to "criminalize" the Internet, but never later argues those attacks have anything to do with the merits of Noom's motion. *See* N.D. Cal. Guidelines for Professional Responsibility, Section 7. Plaintiffs therefore simply note that they respectfully disagree with Noom's attacks.

LEGAL STANDARD

A court may dismiss a complaint under Fed. R. Civ. P. 12(b)(6) when it does not contain enough facts to state a claim to relief that is plausible on its face. *See Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 570 (2007). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). "The plausibility standard is not akin to a 'probability requirement,' but it asks for more than a sheer possibility that a defendant has acted unlawfully." *Amcor Flexibles Inc. v. Fresh Express Inc.*, 2014 WL 2967909, at *3 (N.D. Cal. July 1, 2014) (Beeler, J.) (quoting *Iqbal*, 556 U.S. at 678). "In considering a motion to dismiss, a court must accept all of the plaintiff's allegations as true and construe them in the light most favorable to the plaintiff." *Id.*, at *4.

"When lack of standing pertains to a federal court's subject-matter jurisdiction under Article III, it is properly raised in a motion to dismiss under Federal Rule of Civil Procedure 12(b)(1)." *Torrey Pines Logic, Inc. v. Gunweks, LLC*, 2020 WL 6321569, at *2 (S.D. Cal. Oct. 28, 2020) (internal quotations omitted). "A defendant's Rule 12(b)(1) jurisdictional attack can be either facial or factual." *Antman v. Uber Techs., Inc.*, 2015 WL 6123054, at *4 (N.D. Cal. Oct. 19, 2015) (Beeler, J.). "A 'facial' attack asserts that a complaint's allegations are themselves insufficient to invoke jurisdiction, while a 'factual' attack asserts that the complaint's allegations, though adequate on their face to invoke jurisdiction, are untrue." *Id.* (internal quotations omitted). If a defendant brings a facial challenge, "a court must accept[] all allegations of fact in the complaint as true and construe[] them in the light most favorable to the plaintiffs." *Id.* (citing *Warren v. Fox Family Worldwide, Inc.*, 328 F.3d 1136, 1139 (9th Cir. 2003)).

ARGUMENT

I. PLAINTIFFS SUFFICIENTLY ALLEGE A CLAIM UNDER § 631

A. The Text Of § 631, *Moosejaw*, And *In Re Facebook* Establish That Noom May Be Liable For Enabling FullStory's Wiretapping

Noom argues it "should not be held liable under any aiding and abetting theory of liability because it was a party to the communication with Plaintiffs." MTD at 7:4-5. The plain text of § 631, as well as caselaw, establishes Noom can be liable for enabling FullStory's eavesdropping.[2]

Statutory interpretation begins "with the language of the statute itself." *Harris v. Harris*, 935 F.3d 670, 673 (9th Cir. 2019); *accord In re Hulu Privacy Litig.*, 2012 WL 3282960, at *5 (N.D. Cal. Aug. 10, 2012) (Beeler, J.). Section 631 not only prohibits eavesdropping, but also imposes liability for "*any person*" who "aids, agrees with, employs, or conspires with" anyone who violates section 631(a). Cal. Penal Code § 631(a) (emphasis added); *see also In re Lenovo Adware Litig.*, 2016 WL 6277245, at *8 (N.D. Cal. Oct. 27, 2016) (denying motion to dismiss § 631 claim based solely on allegation that the defendant "aided, agreed with, or conspired with" another defendant to violate section 631). Section 631(a) includes no exemption for participants to a conversation who permit third parties to eavesdrop on that conversation. *See* Cal. Penal Code § 631(a). In other contexts, the Ninth Circuit and California Supreme Court have held that the term "'[a]ny person' means exactly that, and may not be interpreted restrictively." *Bonnichsen v. United States*, 367 F.3d 864, 874 (9th Cir. 2004); *see People v. Snyder*, 22 Cal. 4th 304, 314 (2000) ("[W]e entertain no doubt that the reference to 'any person' in section 84301 should be construed according to its plain and obvious meaning."). There is no reason for a different interpretation here. That same principle applies here because "the California Supreme Court's repeated finding that the California legislature intended for CIPA to establish broad privacy protections supports an expansive reading of the statute." *In re Google Inc.*, 2013 WL 5423918, at *21 (N.D. Cal. Sept. 26, 2013).

[2] Citing *Rogers v. Ulrich*, 52 Cal. App. 3d 894 (1975) and *Membrila v. Receivables Performance Mgmt.*, 2010 WL 1407274 (S.D. Cal. Apr. 6, 2010), Noom also argues it cannot be directly liable in the absence of aiding and abetting liability. As was the case in *Moosejaw*, Plaintiffs' § 631(a) claim against Noom is premised solely on aiding and abetting liability. *See* FAC ¶ 36-39, 72; *see also Moosejaw*, 2019 WL 5485330 at *2.

Judge Chhabria's decision in *Revitch v. New Moosejaw, LLC*, 2019 WL 5485330 (N.D. Cal. Oct. 23, 2019) ("*Moosejaw*") is instructive because it involves the same facts and issues presented here. Like here, a website operator (Moosejaw.com) hired a third party (NaviStone) to "eavesdrop[] on [plaintiff's website] communications with Moosejaw." *Moosejaw*, 2019 WL 5485330, at *1. The *Moosejaw* court rejected the same argument Noom makes here because even if Moosejaw could not be liable for eavesdropping on its own communications, it could still be liable under section 631 for "enabling NaviStone's wrongdoing." *Id.* at *2.

The *Moosejaw* court followed the California Supreme Court's decision in *Ribas v. Clark*, 38 Cal. 3d 355 (1985), which held that § 631 "was designed to protect a person placing or receiving a call from a situation where the person on the other end of the line permits an outsider to tap his telephone *or listen* in on the call." *Ribas*, 38 Cal. 3d at 363 (emphasis in original). "Allow[ing] third persons to eavesdrop on conversations via extensions would be a clear contradiction of the intent of section 631(a)." *Id.* That reasoning applies here because Noom "aids, agrees with, employs, or conspires with" FullStory to eavesdrop on communications on noom.com. *See* FAC ¶¶ 66, 72 (aiding and abetting allegations); *see also id.* at ¶¶ 35-40.

Further, the Ninth Circuit rejected the same argument Noom advances here in *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589 (9th Cir. 2020) ("*In re Facebook III*"). There, the Ninth Circuit explained the intent of wiretap laws is to "prevent the acquisition of the contents of a message by an *unauthorized third-party or an unseen auditor*"—like FullStory here.[3] *In re Facebook III*, 956 F.3d at 608 (emphasis added); *see also id.* at 598 (explaining similar legislative purposes behind CIPA and the federal Wiretap Act). "Permitting an entity to engage in the unauthorized duplication and forwarding of unknowing users' information would render permissible the most common methods of intrusion, allowing the exception to swallow the rule.

[3] FullStory admits several times in its brief that it is a third party to the communications. *See* FullStory's Motion to Dismiss the First Amended Complaint, ECF No. 35, at 14:17 (describing FullStory as a " third part[y]"); *id.* at 15:5-6 ("Noom and Noom's *third-party service providers* may use a variety of technologies that *automatically* (or passively) store or collect certain information.") (emphasis in original); *id.* at 15:14-17 ("The code is temporarily downloaded onto User's Device from Noom's web server and/or Mobile App or a *third party service provider*") (emphasis in original). Noom's brief admits to the same. Noom agrees with this characterization in its own brief. *See* MTD 2:1-3 (comparing FullStory to a "safety consultant" and a "theft detection expert").

Therefore, we conclude that Facebook is not exempt from liability as a matter of law under the Wiretap Act or CIPA as a party to the communication." *Id*.

The same reasoning applies here. This case and *In re Facebook III* both involve website operators who surreptitiously record information about consumer's internet usage and activity. *See* FAC ¶¶ 1, 17-27. This case involves "the acquisition of the contents of a message by an unauthorized third-party or an unseen auditor"—namely, FullStory. *In re Facebook III*, 956 F.3d at 608; *see also* FAC ¶¶ 17-33 (describing FullStory's software). The amount of information Defendants monitor is more extensive here than it was in *In re Facebook III*: Facebook only tracked website user's internet history. *See In re Facebook III*, 956 F.3d at 603. Here, Defendants not only monitor what webpages a visitor looks at, but also everything they do while on the webpage, including the entry of medical and health information. *Compare In re Facebook III*, 956 F.3d at 596, *with* FAC ¶¶ 19, 23, 25, 30, 46, 55. In sum, adopting Noom's argument would be reversible error under *In re Facebook III*.[4]

None of Noom's authorities support dismissal. Noom primarily relies on *Powell v. Union Pac. Railroad Co.*, 864 F. Supp. 2d 949 (E.D. Cal. Mar. 31, 2012), for the proposition that a party to a communication cannot be liable for aiding and abetting under § 631. But the *Powell* court did *not* hold that a party to a communication can *never* be liable for aiding and abetting unlawful eavesdropping, as Noom implies. *See Powell*, 864 F. Supp. 2d at 955-56. Instead, *Powell* concluded there was no "third party" present when two Union Pacific officers who were jointly conducting a company investigation participated in a phone call with another Union Pacific employee. *See id*. at 953 (describing circumstances of eavesdropping claim); *id.* at 954-56 (explaining legal basis for the decision). It logically follows that if there was no "third party" in the first place, then there was no basis to find the defendant "aided" in the violation of § 631 by a third party. Noom's expansive interpretation of *Powell* cannot be squared with the plain text of

[4] Noom resorts to hyperbole by claiming liability here would "expose vast swaths of website operators to criminal liability, and cause serious repercussions for the basic functionality of the Internet." MTD at 2:4-5. That is not a legal argument for dismissal. In any event, Plaintiff alleges that the technology at issue here is *not* normal, socially accepted, or safe. FAC ¶¶ 28, 34, 55.

§ 631 or the later controlling decision in *In re Facebook III*, and in any event, the facts in *Powell* are easily distinguishable here.

Noom also cites *Kirch v. Embarq Management Co.*, 702 F.3d 1245 (10th Cir. 2012) for the proposition that the language of the *federal* Wiretap Act includes no aiding and abetting liability. That is beside the point because CIPA does. *Compare* Cal. Penal Code § 631(a), *with* 18 U.S.C.A. § 2520; *see also In re Lenovo Adware Litig.*, 2016 WL 6277245 at *8 (addressing aiding and abetting liability under CIPA); *Moosejaw*, 2019 WL 5485330 at *2 (same).

B. Plaintiffs' Website Interactions Are "Communications" Under *Moosejaw*, *In re Facebook*, And *In re Zynga*

In a footnote, Noom makes a half-developed argument that "most if not all of" the data Defendants intercepted are not "'electronic communications' within the meaning of Section 631." MTD at 8 n.2 (referring to "mouse clicks," "keystrokes" and "payment card information"). The argument was footnoted because it lacks merit. As stated in Section I.A above, in *Moosejaw*, 2019 WL 5485330, at *1-2, the district court denied a motion to dismiss claims under § 631 where, like here, a website hired a third-party technology company to monitor website visitors' mouse clicks, keystrokes, and other website activities. The district court held "[plaintiff's] interaction with the Moosejaw website is communication within the meaning of section 631." *Moosejaw*, 2019 WL 5485330, at *1; *see also Luis v. Zang*, 833 F.3d 619, 624 (6th Cir. 2016) (plaintiff sufficiently alleged claim under federal Wiretap Act based on use of "WebWatcher" software that "records all PC activity including emails, IMs, websites visited, web searches, Facebook/MySpace activity, and anything typed in real time.").

The outcome in *Moosejaw* is supported by two Ninth Circuit decisions addressing the federal Wiretap Act and CIPA.[5] Last year, the Ninth Circuit reversed dismissal and held that the collection of website visitors' internet history and search terms supported claims under both CIPA and the federal Wiretap Act, as they "divulge a user's personal interests, queries, and habits on third party websites." *In re Facebook III*, 956 F.3d at 604-606. Even URL addresses may qualify

[5] The analysis of whether something is the "contents" of a communication under CIPA is generally the same as it is under the federal Wiretap Act. *Brodsky v. Apple Inc.*, 445 F. Supp. 3d 110, 127 (N.D. Cal. 2020).

as "content" because they reveal "'the particular document within a website that a person views.'" *Id.* at 605 (quoting *United States v. Forrester*, 512 F.3d 500, 510 n.6 (9th Cir. 2008)).

Prior to *In re Facebook III*, the Ninth Circuit explained that the First Circuit had "correctly concluded" that "the content of the sign-up information customers provided to pharmaceutical websites, which included their 'names, addresses, telephone numbers, email addresses, dates of birth, genders, insurance statuses, education levels, occupations, medical conditions, medications, and reasons for visiting the particular website'" were actionable communications under the federal Wiretap Act. *In re Zynga Privacy Litig.*, 750 F.3d 1098, 1107 (9th Cir. 2014) ("*In re Zynga*") (quoting *In re Pharmatrak, Inc.*, 329 F.3d 9, 18 (1st Cir. 2003)). "[S]earch term[s] or similar communication[s] made by the user" on the internet also qualify as "content." *Id*. at 1109. District courts have found a wide array of communications are covered by the Wiretap Act or CIPA, ranging from Facebook "likes" to remotely activated changes to device settings. *See Rainsy v. Facebook, Inc.*, 311 F. Supp. 3d 1101, 1115 (N.D. Cal. 2018); *S.D. v. Hytto Ltd.*, 2019 WL 8333519, at *7 (N.D. Cal. May 15, 2019) ("*Hytto*").

Here, the information captured by Defendants' wiretapping falls within the range of information covered by the above-cited authorities. The FAC is based on admissions by FullStory that it records not only which webpages a user visits, but also everything a user does on those webpages, everything they search for, and all the information they provide. *See* FAC ¶¶ 19-29.

Noom's arguments on this issue do not support dismissal for three reasons. First, Noom does not make any argument for dismissal to the extent the claims are based on monitoring which webpages a user visits or searches for (covered by *In re Facebook III* and *Moosejaw*), or a user's health information (such as height and weight, gender, age range, diet and exercise habits, or health conditions), which is covered by *In re Zygna*.

Second, Noom mistakenly cites *In re Zynga* for the proposition that "mouse clicks," "keystrokes" and "payment card information" are not "contents" that can support a claim here. MTD at 8 n.2. That interpretation is contradicted by the holding of *In re Zynga*, which as noted above supports Plaintiffs' position. *See In re Zynga*, 750 F.3d at 1107. Noom's position stems from a misunderstanding of the term "record information," which generally does not qualify as

"content." *Hytto*, 2019 WL 8333519, at *6. "Record information is typically data *generated automatically* at the sending of the message and is incidental to the use of the communication device." *Id.* (emphasis added). "Unlike record information, content is generated not automatically, but through the intent of the user." *Id.* Thus, for example, if someone types in the body of an email that her name is "Jane Doe," then that information qualifies as "content"; whereas the automatic appearance of her name in the email "From" line might not. *See In re Zynga*, 750 F.3d at 1107 (discussing distinction between information typed in an email messages as opposed to "automatically generated" information, and explaining that name, address, and other information provided by website visitors in form fields are "content").

Here, there are no allegations that "mouse clicks," "keystrokes" and "payment card information" of website visitors are automatically generated, and it would be improper on a 12(b)(6) motion to draw such an inference against the Plaintiff. *See Koala v. Khosla*, 931 F.3d 887, 894 (9th Cir. 2019) (addressing standard on 12(b)(6) motion). It is common experience that website users provide payment information or click on buttons when purchasing services on the Internet, just like the customers who provided their information on the pharmaceutical website referenced in *In re Zynga*, 750 F.3d at 1107. Even if Noom is correct that such information is *automatically generated* such that it qualifies qualify as "record information," that is not a basis to dismiss the entire claim given that Noom does not dispute that certain website interactions and health information qualify as content. *See Hytto*, 2019 WL 8333519, at *7.

II. PLAINTIFFS SUFFICIENTLY ALLEGE A CLAIM UNDER CIPA § 635

A. Plaintiffs Have Both A Private Right Of Action And Standing To Assert A Claim Under § 635

In two related arguments, Noom argues "Plaintiffs lack both constitutional and statutory standing to pursue a Section 635 claim because CIPA's private right of action cannot be extended to permit suits predicated on the mere 'possession' of an alleged eavesdropping device." MTD at 8:17-19. That is wrong.

Noom's argument that Plaintiffs lack a private right of action contradicts the text of the statute. Section 635 imposes liability on "[*e*]*very person* who … *possesses* … or furnishes to

another *any device* which is primarily or exclusively designed or intended for eavesdropping." Cal. Penal Code § 635 (emphasis added). Section 637.2 provides that "it is not a necessary prerequisite to an action pursuant to this section that the plaintiff has suffered, or been threatened with actual damages." *Ion Equip. Corp. v. Nelson*, 110 Cal. App. 3d 868, 882 (1980); *see also* Cal. Penal Code § 637.2(b) (permitting any person to "bring an action to enjoin and restrain any violation of this chapter, *and may in the same action seek damages as provided by subdivision (a)*") (emphasis added). Thus, as was held in *Moosejaw*, there is a private right of action under § 635. *Moosejaw*, 2019 WL 5485330, at *3 (denying motion to dismiss § 635 claim). Defendants cite no contrary authority involving claims under CIPA.

Equally meritless is Noom's argument that Plaintiffs lack standing under *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540 (2016). MTD at 8:21-9:11. The court in *Moosejaw* rejected the same argument, based on the same authority, when it held that the plaintiff in that case had standing to assert a claim under § 635. *Moosejaw*, 2019 WL 5485330 at *1. The court first explained that wiretapping is "not at all like the sort of 'bare procedural violation' that the Supreme Court has said [in *Spokeo*] would fall short of an Article III injury," and then explained that plaintiff "alleged injuries traceable to Moosejaw's possession and use of the [internet monitoring] device." *Id.*, at *1, *3. Moreover, the Ninth Circuit has held that wiretapping claims—including under CIPA—are sufficient to confer Article III standing under *Spokeo*. *See In re Facebook III*, 956 F.3d at 599 (holding "Plaintiffs have adequately alleged an invasion of a legally protected interest that is concrete and particularized" based on an alleged violation of CIPA); *see Romero v. Securus Techs., Inc.*, 216 F. Supp. 3d 1078, 1088 (S.D. Cal. 2016) (rejecting Defendants' same argument, holding that "[a] violation of CIPA involves much greater concrete and particularized harm than a technical violation of the Fair Credit Reporting Act ('FRCA'), the statute at issue in *Spokeo*.").

Standing is also supported by the Sixth Circuit's decision in *Luis v. Zang*, 833 F.3d 619 (6th Cir. 2016), which involved a claim under § 2512(b), a provision of the federal Wiretap Act that similarly prohibits the possession of wiretap devices. *See* 18 U.S.C. § 2512(b) (imposing liability on any person who "manufactures, assembles, [or] possesses …" wiretapping devices). The *Luis* court first noted a split of authority as to whether mere possession alone could support a claim

under § 2512(b), but ultimately concluded that possession, coupled with "knowledge" and "active[] involve[ment]" with the wiretapping, could support a claim. *Luis*, 833 F.3d at 636-37.

As in *Moosejaw* and *Luis*, Plaintiffs not only allege that Noom possessed a wiretapping device, but also allege Noom's knowledge and active involvement in using that device to monitor their communications. *See* FAC ¶¶ 1, 36-40, 43, 80. Accordingly, Noom's argument that there are "little to no details as to how FullStory's Session Replay technology was purportedly deployed" overlooks Plaintiffs' allegations. MTD at 9:5-7.

B. Fullstory's Code Is A "Device" That Is "Primarily Or Exclusively" Designed For Eavesdropping

Next, relying on *In re Facebook Internet Tracking Litig.*, 263 F. Supp. 3d 836 (N.D. Cal. 2017) ("*In re Facebook II*"), Noom argues "Plaintiffs fail to allege sufficient facts to show the alleged 'code' installed on Noom's website is a device 'primarily or exclusively designed for eavesdropping." MTD at 10:20-21. That is wrong.[6]

Plaintiffs allege that "FullStory's code is a 'device' that is 'primarily or exclusively designed' for eavesdropping. That is, FullStory's code is designed to gather PII, including keystrokes, mouse clicks, and other electronic communications." FAC ¶ 81.[7] Nothing more is required. *See Moosejaw*, 2019 WL 5485330, at *3 ("At the pleading stage, the Court must assume the truth of Revitch's allegation that NaviStone's code is a device … primarily or exclusively designed or intended for eavesdropping upon the communication of another.") (internal quotations omitted). And there are ample allegations in the FAC describing the functionality and purpose of FullStory's code, supported by many quotes and images from FullStory describing its code. FAC ¶¶ 19-33.

[6] Notably, the portion of *In re Facebook II* quoted by Noom concerned whether the plaintiffs "established that they ha[d] a reasonable expectation of privacy in the URLs of the pages they visit[ed]" – it was not in the context of a Section 635 claim. *In re Facebook II*, 263 F. Supp. 3d at 846. Accordingly, Noom's argument that the software "allegedly behaves and is used in a manner identical to any technology designed to facilitate web-browsing activity," is inapposite. MTD at 11:10-11. This argument is also belied by Plaintiffs' allegations. FAC ¶¶ 28, 34, 55.

[7] For this reason, Noom's argument that Plaintiffs "do not explain why that function makes it a device 'primarily or exclusively designed' for *eavesdropping*" is meritless.

In any event, courts have rejected the same or similar arguments raised by Noom because they rest on factual disputes about how the defendant's technology operates. *See Moosejaw*, 2019 WL 5485330, at *3 (the question of whether defendant's internet tracking technology was a wiretap "device" under § 635 of CIPA is a question of fact); *cf. In re Carrier IQ, Inc.*, 78 F. Supp. 3d 1051, 1082 (N.D. Cal. 2015) ("[E]ven if the Defendants are factually correct that the communications at issue in this case were in transitory storage on Plaintiffs' mobile devices … it is not at all apparent why there was no 'captur[ing] or redirect[ing]' of these communications contemporaneous with their transmission.").

III. DISMISSAL OF THE INVASION OF PRIVACY CLAIM WOULD BE REVERSIBLE ERROR UNDER *IN RE FACEBOOK III*

1. Legally Protected Privacy Interest

Noom asks this Court to determine as a matter of law, upon the pleadings and without a developed factual record, that PII and PHI—including health, dieting, and medical information—cannot ever legally constitute "information subject to constitutional protection." MTD at 13:15-19. Noom's argument is belied by Plaintiffs' allegations and by the Ninth Circuit's decision in *In re Facebook III*. As detailed below, Plaintiffs sufficiently allege an invasion of a legally protected privacy interest.[8]

Plaintiffs allege FullStory, with Noom's consent and participation, surreptitiously collected and stored highly sensitive PII and PHI in real time. FAC ¶ 1; *see also id.* ¶ 45 ("When users access Defendant Noom's website, they fill out a form and enter PII and PHI. FullStory's software captures these electronic communications throughout each step of the process. Even if users do not complete the form, the Website nonetheless captures users' electronic communications throughout his or her visit."); *id.* ¶ 46 (listing categories of information collected, including history of medical conditions, diet and exercise habits, and user location, among others). By amassing Plaintiffs' and

[8] The California Supreme Court has at times described "[l]egally recognized privacy interests as generally" falling in two classes: "information privacy" and "autonomy privacy." Both privacy interests are at stake here. "Informational privacy" is at issue because Plaintiffs allege Noom "misuse[d] [their] sensitive, confidential PII and PHI." FAC ¶ 87. Likewise, "autonomy privacy" is at issue because Noom's comprehensive tracking and collection of Plaintiffs' electronic communications restricts Plaintiffs' ability to "mak[e] personal decisions . . . without observation [or] intrusion." *Hill*, 7 Cal. 4th at 35; *see also* FAC ¶ 87.

Class members' PII and PHI, Noom has divested them of the ability to "mak[e] intimate personal decisions or conduct[] personal activities without observation [or] intrusion." *Hill v. Nat'l Collegiate Athletic Assn.*, 7 Cal. 4th 1, 35 (1994); *see also McDonald v. Kiloo ApS*, 2019 WL 2211316, at *4 (N.D. Cal. May 22, 2019) ("Current privacy expectations are developing, to say the least," and thus "privacy interest and accompanying legal standards are best viewed flexibly and in context.").

Against the weight of this precedent, Noom relies on a case rejecting the argument that a criminal sex offender had a superior interest in protecting the privacy of his home address than the State did in providing notice of it to protect the public. MTD at 13:22-24 (citing *Fredenburg v. City of Fremont*, 119 Cal. App. 4th 408, 423 (2004)). The location information at issue in *Fredenburg* was limited to the "general location of one's residence," and did not extend to the surreptitious collection of PII and PHI.[9]

As a last-ditch effort, Noom argues that "Plaintiffs do not plead, as they must, that the information they provided to Noom was 'disseminated' or 'misused' in any fashion." MTD at 14:5-6. Not so. Plaintiffs allege that Noom collected their PII and PHI in real time and shared it with FullStory, unbeknownst to Plaintiffs and Class members. FAC ¶¶ 4-5 (Plaintiffs were "unaware at the time that [their] keystrokes, mouse clicks, and other electronic communications, including the information described above, were being intercepted in real-time and would be disclosed to FullStory, nor did [they] consent to the same.").

2. Reasonable Expectation of Privacy

Noom argues Plaintiffs "do not allege conduct consistent with an expectation of privacy" because "nowhere do Plaintiffs claim they had an actual expectation that their activity was or should be hidden *from Noom*." MTD at 14:23-28. That misses the point. This is a wiretapping case, and Plaintiffs sufficiently allege they did not know that a *third party*—FullStory—was

[9] Noom's reliance on *In re Yahoo Mail Litig.*, 7 F. Supp. 3d 1016 (N.D. Cal. 2014) is misplaced because "[u]nlike in *In re Yahoo Mail Litigation*, Plaintiffs identify a discrete type of sensitive information … that is legally protected, rather than arguing they have a legally protected interest in a method of communication." *In re Vizio, Inc., Consumer Privacy Litig.*, 238 F. Supp. 3d 1204, 1232 (C.D. Cal. 2017) ("*In re Vizio*").

secretly recording their interactions with Noom's website without Plaintiffs' consent. FAC ¶¶ 4-5 ("Plaintiffs allege that they were "unaware at the time that [their] keystrokes, mouse clicks, and other electronic communications, including the information described above, were being intercepted in real-time and would be disclosed to FullStory, nor did [they] consent to the same."), *see also id.* ¶ 47 ("Users are never told that their electronic communications are being wiretapped by FullStory). Plaintiffs' allegations are bolstered by caselaw. *See In re Facebook III*, 956 F.3d at 603 ("In light of the privacy interests and Facebook's allegedly surreptitious and unseen data collection, Plaintiffs have adequately alleged a reasonable expectation of privacy. Case law supports this determination."); *In re Google Location History Litig.*, 2021 WL 519380, at *6 (N.D. Cal. Jan. 25, 2021) ("Courts have held that plaintiffs have a reasonable expectation of privacy where data is collected without their consent."). The Ninth Circuit has also held that "[t]he nature of the allegedly collected data is also important." *In re Facebook III*, 956 F.3d at 603. This holds especially true here given Plaintiffs allege Noom has collected personal health information, including medical history and dieting information. FAC ¶ 46.

Noom also argues that Plaintiffs should have known they were being wiretapped because "virtually all consumer-facing websites track the conduct of web visitors for myriad reasons" and that such a practice is "near-universal." MTD at 15:10-12. This argument raises questions of fact that are inappropriate for resolution on the pleadings. *See Hill*, 7 Cal. 4th at 40 ("Whether plaintiff has a reasonable expectation of privacy in the circumstances and whether defendant's conduct constitutes a serious invasion of privacy are mixed questions of law and fact."); *see also In re Facebook III*, 956 F.3d at 603 ("In light of the privacy interests and Facebook's allegedly surreptitious and unseen data collection, Plaintiffs have adequately alleged a reasonable expectation of privacy."). Regardless, Plaintiffs allege they did not know and could not have known they were being wiretapped, and that Session Replay technologies are not ubiquitous or common. FAC ¶¶ 55-56 ("[T]he extent of data collected by these services far exceeds user expectations … Neither Plaintiffs nor any Class member consented to being wiretapped on the Website, or to have their communications recorded and shared with FullStory."); *see also id.* at ¶¶ 1, 4-5, 28, 34, 47-54. These allegations underscore why Noom's argument is a question of fact.

3. Highly Offensive

Noom argues "[e]ven if Plaintiffs had a legally protectable and objectively reasonable expectation that no party could view their activity on Noom's website, Noom's alleged monitoring would still not be highly offensive or meet the 'high bar' for a common law invasion of privacy claim." MTD at 15:15-17. That is wrong.

As an initial matter, "California tort law provides no bright line on ['offensiveness']; each case must be taken on its facts." *Hernandez v. Hillsides, Inc.*, 47 Cal. 4th 272, 287 (2009) (quoting *Shulman v. Group W Prods., Inc.,* 18 Cal. 4th 200, 237 (1998)). Indeed, collection of intimate or sensitive personally identifiable information may amount to a highly offensive intrusion. *See*, *e.g.*, *Goodman v. HTC Am., Inc.*, 2012 WL 2412070, at *14-15 (W.D. Wash. June 26, 2012); *In re Vizio*, 238 F. Supp. 3d at 1233 (same). Notably, Plaintiffs allege that Defendants wiretapped their electronic communications surreptitiously (FAC ¶¶ 47, 90), and "courts have held that 'deceit can be a kind of 'plus' factor [that is] significant in ... making a privacy intrusion especially offensive.'" *In re Google Location History Litig.*, 2021 WL 519380, at *7 (N.D. Cal. Jan. 25, 2021) (quoting *Heeger v. Facebook, Inc.*, 2019 WL 7282477, at *4 (N.D. Cal. Dec. 27, 2019)); *accord McDonald*, 385 F. Supp. 3d at 1036.

Ultimately, however, whether Noom's conduct was sufficiently offensive raises a question of fact. *See In re Google Location History Litig.*, 2021 WL 519380, at *7 ("Whether Google's collection and storage of location data when Location History was set to off was highly offensive to a reasonable person is a question of fact."). On that basis, the Ninth Circuit reversed dismissal of an invasion of privacy claim where Facebook only obtained internet history—which is far less than the scope of information obtained here. *See In re Facebook III*, 956 F.3d at 606 ("The ultimate question of whether Facebook's tracking and collection practices could highly offend a reasonable individual is an issue that cannot be resolved at the pleading stage."); *see also Moosejaw*, 2019 WL 5485330, at *3 (denying motion to dismiss because whether conduct is offensive is a factual question); *Opperman v. Path, Inc.*, 205 F. Supp. 3d 1064, 1079 (N.D. Cal. 2016) ("*Opperman II*") (same). Thus, Noom asks the Court to make the same reversible error made in *In re Facebook III*.

Noom primarily relies on *Folgestrom v. Lamps Plus, Inc.*, 195 Cal. App. 4th 986 (Cal. Ct. App. 2011), but *Foglestrom* does not support Noom's position. As Judge Tigar explained in *Opperman v. Path, Inc.*, 87 F. Supp. 3d 1018 (N.D. Cal. 2014) ("*Opperman I*"), *Folgestrom* is "distinguishable" because it did not involve the "surreptitious" acquisition of personal information. Judge Tigar likewise rejected the argument that secretly acquiring personal information, like Noom has done here, is "routine commercial behavior," and concluded that whether the conduct at issue was "highly offensive" was a factual dispute "best left for a jury." *Opperman I*, 87 F. Supp. 3d at 1061; *see also In re Facebook, Inc., Consumer Privacy User Profile Litig.*, 402 F. Supp. 3d 767, 797 (N.D. Cal. 2019) ("Under California law, courts must be reluctant to reach a conclusion at the pleading stage about how offensive or serious the privacy intrusion is.").

Judge Tigar also declined to follow *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040 (N.D. Cal. 2012) ("*In re iPhone*"), explaining he was "not persuaded by cases that have mechanically applied *Folgelstrom* to invasion of privacy claims." *Opperman II*, 205 F. Supp. 3d at 1078. As Judge Tigar explained:

> [*In re iPhone Application Litigation*] involved the disclosure to third parties of an iDevice user's unique device identifier number, personal data, and geolocation information. … That court held without explanation that "[e]ven assuming this information was transmitted without Plaintiffs' knowledge and consent, a fact disputed by Defendants, such disclosure does not constitute an egregious breach of social norms," citing *Folgelstrom*. *Id.* As noted above, however, *Folgelstrom* addressed different facts than those in *iPhone Application Litigation*, and the latter court did not explain how expansion of *Folgelstrom's* holding, counter to the privacy interests of iDevice users, was consistent with California's community privacy norms.

Id. at 1078-79 (emphasis added).

Opperman I and *II*'s critique of cases that extended *Folgelstrom* too far also applies to two other decisions cited by Noom that followed *Folgelstrom*: *Yunker v. Pandora Media, Inc.*, 2013 WL 1282980 (N.D. Cal. Mar. 26, 2013), and *In re Google Android Consumer Privacy Litig.*, 2013 WL 1283236 (N.D. Cal. Mar. 26, 2013). *In re Google Android Consumer Privacy Litig.* is particularly inapposite because the facts at issue here are more akin to the *Opperman* decisions.

See also Goodman v. HTC Am., Inc., 2012 WL 2412070, at *14 (W.D. Wash. June 26, 2012) (privacy violation found when defendant "transmitted user data to a third-party tracking company").

IV. PLAINTIFF MOISE MAY SEEK INJUNCTIVE RELIEF

As to Plaintiff Moise, Noom's argument for dismissal of the request for injunctive relief contradicts *Davidson v. Kimberly-Clark Corp.*, 889 F.3d 956 (9th Cir. 2018), where the Ninth Circuit rejected the defendant's standing arguments and reversed dismissal of a claim seeking injunctive relief.[10] The Ninth Circuit held, in the context of a false advertising case, that a plaintiff's knowledge that they were exposed to wrongful conduct does not foreclose a plaintiff from plausibly alleging that he or she may be exposed to the same conduct by the same defendant in the future. *See Davidson*, 889 F.3d at 969 ("Knowledge that the advertisement or label was false in the past does not equate to knowledge that it will remain false in the future."). Allegations that the plaintiff wanted to continue purchasing the defendant's product, but could not be certain whether the wrongful conduct would continue without injunctive relief were sufficient to support standing. *See id*. at 971-72. The same reasoning applies here. Similar to *Davidson*, Plaintiffs allege as follows:

> Plaintiffs continue to be at risk because they frequently use the internet to search for information about products or services. They continue to desire to use the internet for that purpose, *including for the purpose of shopping for various diets, weight loss plans, or other health-related products*. Defendant FullStory provides its software, including the Session Replay feature, to many other website operators who offer a wide array of services. For many websites that Plaintiffs may or are likely to visit in the future, they have no practical way to know if their website communications will be monitored or recorded by FullStory.

FAC ¶ 75 (emphasis added); *see also id.* at ¶ 83. Noom argues the above allegation is implausible because it does not specify Noom by name. *See* MTD at 17:26 ("[N]owhere do they contend that they intend to use *Noom's* services in the future"). But Plaintiff Moise's interest in using Noom again is reasonably inferred, and at this juncture, the Court is required to "draw[] all reasonable inferences in the plaintiffs' favor." *Whitaker v. Body, Art and Soul Tattoos Los Angeles, LLC*, -- F.

[10] Plaintiff Graham does not seek injunctive relief against Noom.

App'x --, 2021 WL 237321, at *1 (9th Cir. Jan. 25, 2021) (internal quotation omitted); *accord Antman*, 2015 WL 6123054, at *4. If the Court disagrees, then the proper outcome would be leave to amend. *See Cornish v. Oakland Housing Authority*, 2019 WL 1746070, at *2 (N.D. Cal. Apr. 18, 2019) (Beeler, J.) ("If a court dismisses a complaint, it should give leave to amend unless the pleading could not possibly be cured by the allegation of other facts.") (internal quotations omitted).

CONCLUSION

For the foregoing reasons, the Court should deny Defendants' motion to dismiss. If the Court determines that the pleadings are deficient in any respect, Plaintiffs request leave to amend to cure any such deficiencies. *See Roney v. Miller*, 705 F. App'x 670, 671 (9th Cir. 2017) (lower court erred by denying leave to amend after dismissing amended complaint).

Dated: March 5, 2021

Respectfully submitted,

BURSOR & FISHER, P.A.

By: */s/ Joel D. Smith*
Joel D. Smith

L. Timothy Fisher (State Bar No. 191626)
Joel D. Smith (State Bar No. 244902)
1990 North California Blvd., Suite 940
Walnut Creek, CA 94596
Telephone: (925) 300-4455
Facsimile: (925) 407-2700
E-mail: ltfisher@bursor.com
jsmith@bursor.com

Attorneys for Plaintiffs